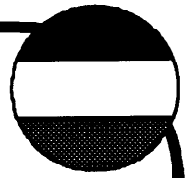
The Army Signal Command



AFCEA Panel: Techniques for Information Assurance

Network Security Improvement Program

Michael L. Gentry, Ph.D.

17 Sep 98

Form SF298 Citation Data

Report Date *("DD MON YYYY")* 17091998	**Report Type** N/A	**Dates Covered (from... to)** *("DD MON YYYY")*

Title and Subtitle AFCEA Panel: Techniques for Information Assurance Network Security Improvement Program Program	**Contract or Grant Number**
	Program Element Number
Authors	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) The Army Signal Command	**Performing Organization Number(s)**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Monitoring Agency Acronym**
	Monitoring Agency Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes	
Abstract	
Subject Terms	
Document Classification unclassified	**Classification of SF298** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** unlimited
Number of Pages 20	

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	9/1/94	Briefing

4. TITLE AND SUBTITLE
AFCEA Panel: Techniques for Information Assurance

5. FUNDING NUMBERS

6. AUTHOR(S)
Michael L. Gentry, Ph.D.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

IATAC
Information Assurance Technology Analysis
Center
3190 Fairview Park Drive
Falls Church VA 22042

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Technical Information Center
DTIC-IA
8725 John J. Kingman Rd, Suite 944
Ft. Belvoir, VA 22060

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

12b. DISTRIBUTION CODE
A

13. ABSTRACT ***(Maximum 200 Words)***

This AFCEA briefing outlines a construct for Techniques for improving information assurance and network security. The security plan is outlined in phases that build the foundation, harden the infrastructure and then insert new technology. The program relies on defense in depth and involves all Army Major Commands (MACOM).

14. SUBJECT TERMS
Network security, information assurance, afcea

15. NUMBER OF PAGES

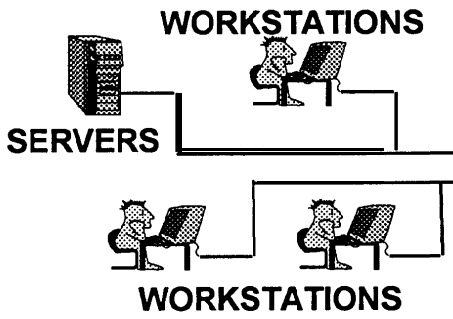
16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	UNCLASSIFIED	UNCLASSIFIED	None

Network Security Improvement Pgm

Phase I

- Workstation and Server-based security
- ID and Passwords
- TCP Wrapper
- Security Scanning
- Anti-Virus

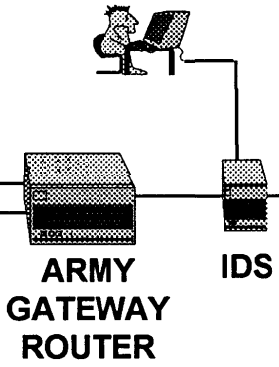


- Training
- World Wide Web Security
- NT Security
- Network Access Policy
- System Policies
- and More ....

Build Foundation

Phase II

- Intrusion Detection System Reporting to DOIM and CERTs
- Router-Based Security (Filtering)

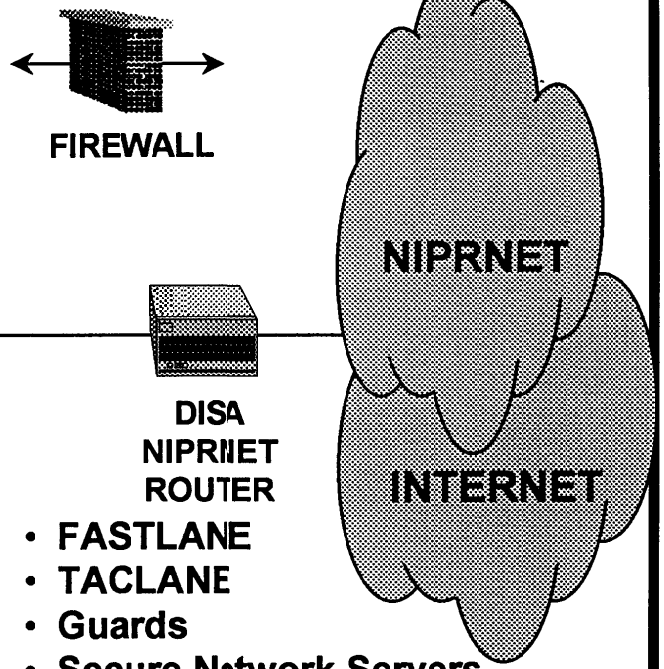


- Centralize Dial-In
- Re-Home Backside Connections
- Security Controls for ISDN Circuits
- Reconfigure Networks

Harden Infrastructure

Phase III

- Install Firewalls (If Needed For Specific Network Security Rqmts
- One-Time Passwords



- FASTLANE
- TACLANE
- Guards
- Secure Network Servers
- Public Key Infrastructure
- Latest technology

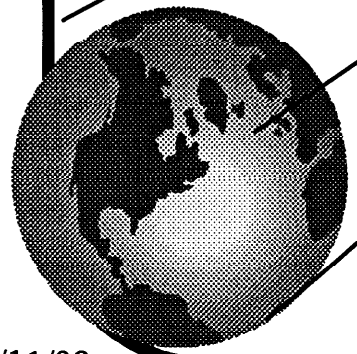
Insert New Technology

C2 Protect VCSA Direction

"...Implement Near-Real-Time (NRT), worldwide, common picture of the Army's Military Information Environment (MIE)

...Combine the Army's Information Service Provider functions with Army Regional Computer Emergency Response Team (RCERT) C2 Protect/ISS services

...Ensure reporting of a common picture of the Army MIE to a central coordination center

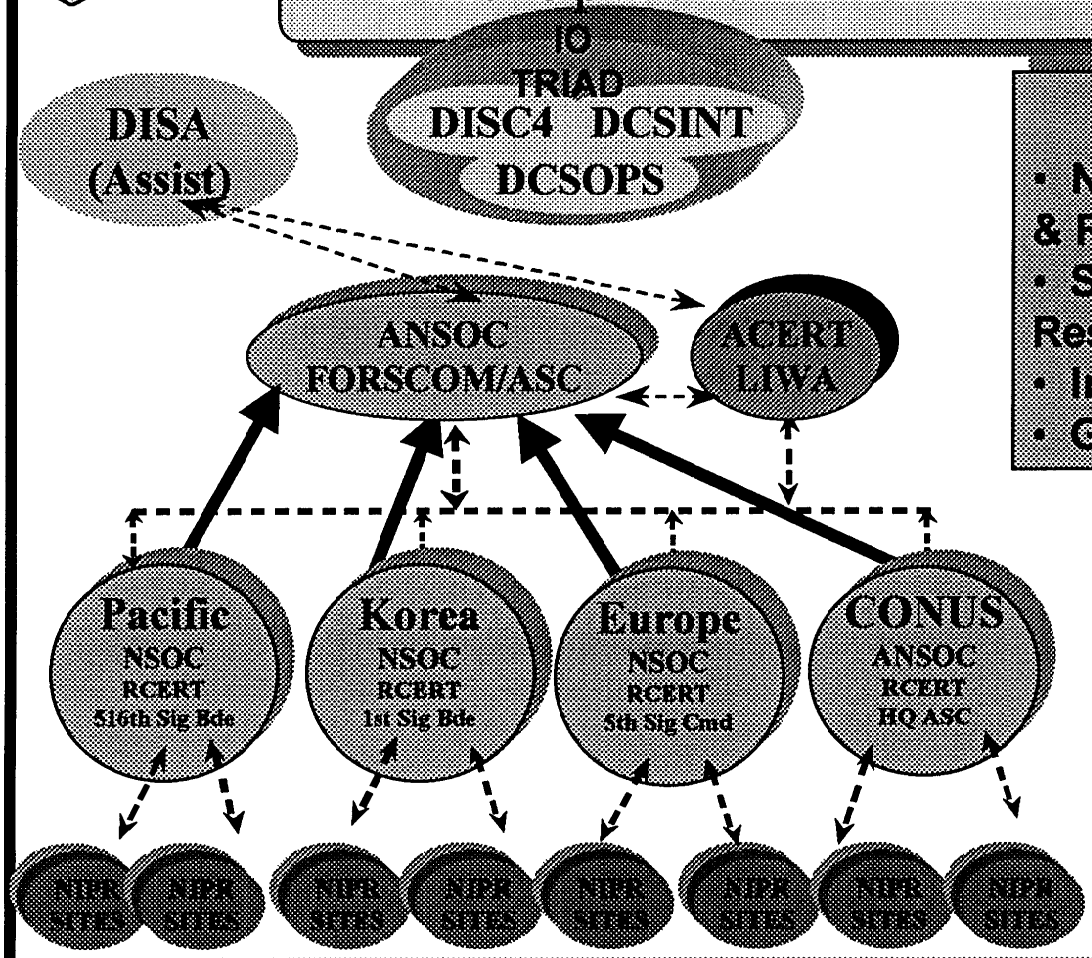


...Enhance acquisition of unified and global NRT protect, detect, and react capabilities through physical integration of functions and virtual collocation at Network & Systems Operation Centers and Regional Computer Emergency Response Teams....." 190904ZFEB98

Focus of Operation INFO GUARD

- **Establish a Hasty Defense for the Sustaining Base information system environment**
  - **Establish intrusion detection on Army NIPRNET connections**
  - **Establish intrusion detection on limited set of high profile Army servers**
  - **Establish a global view of the Army NIPRNET and SIPRNET connectivity**
  - **Establish a protected Army Domain Name Service (DNS) system**
  - **Implement basic configuration management and control capabilities**
- **Prepare plans for a deliberate Defense in Depth starting FY99**

24x7 Operational Forward Presence



ASC

- Networks Operation, Monitor, & Restore
- Systems Operation, Monitor, & Restore
- Integrated C2 Protect
- Global Configuration Control

LIWA

- Analysis
- Info Dissemination
- Coordination/Reporting
- Computer Defense Assessment Program
- Database/tools
- Attack & Response

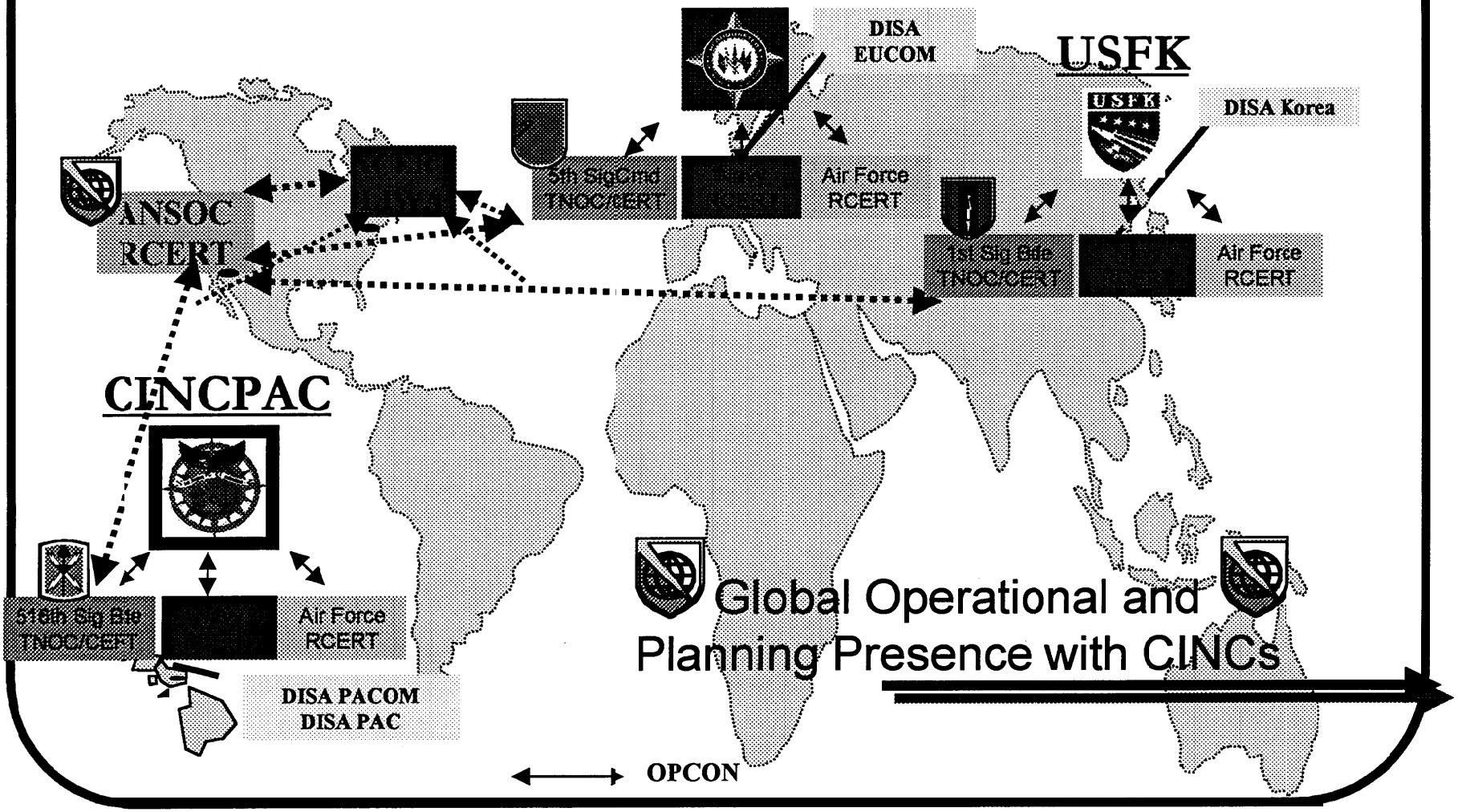
Coordination & Reporting

World Wide Network View

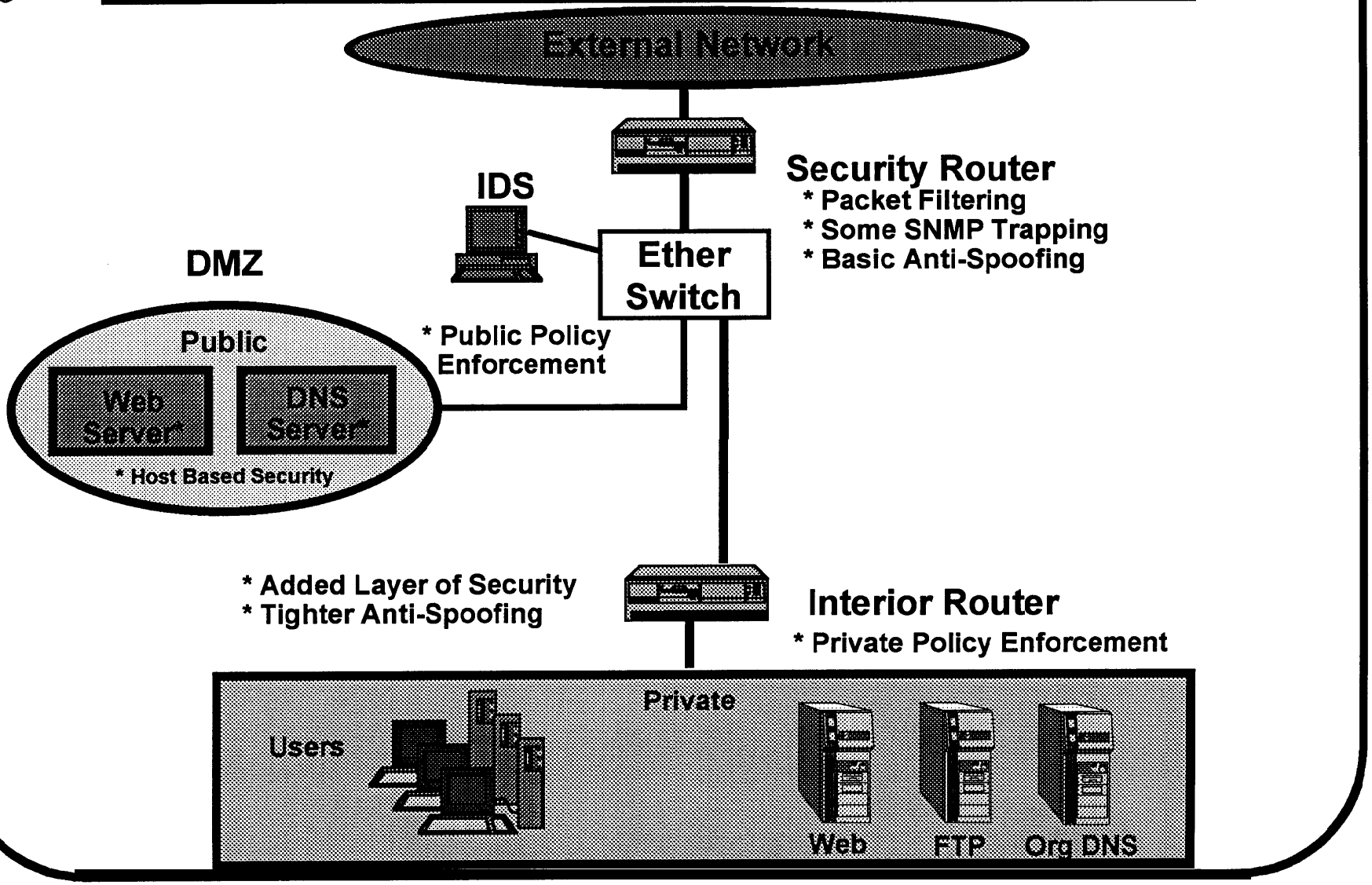
NSOC = Network and Systems Operations Center

RCERT: Regional Computer Emergency Response Team

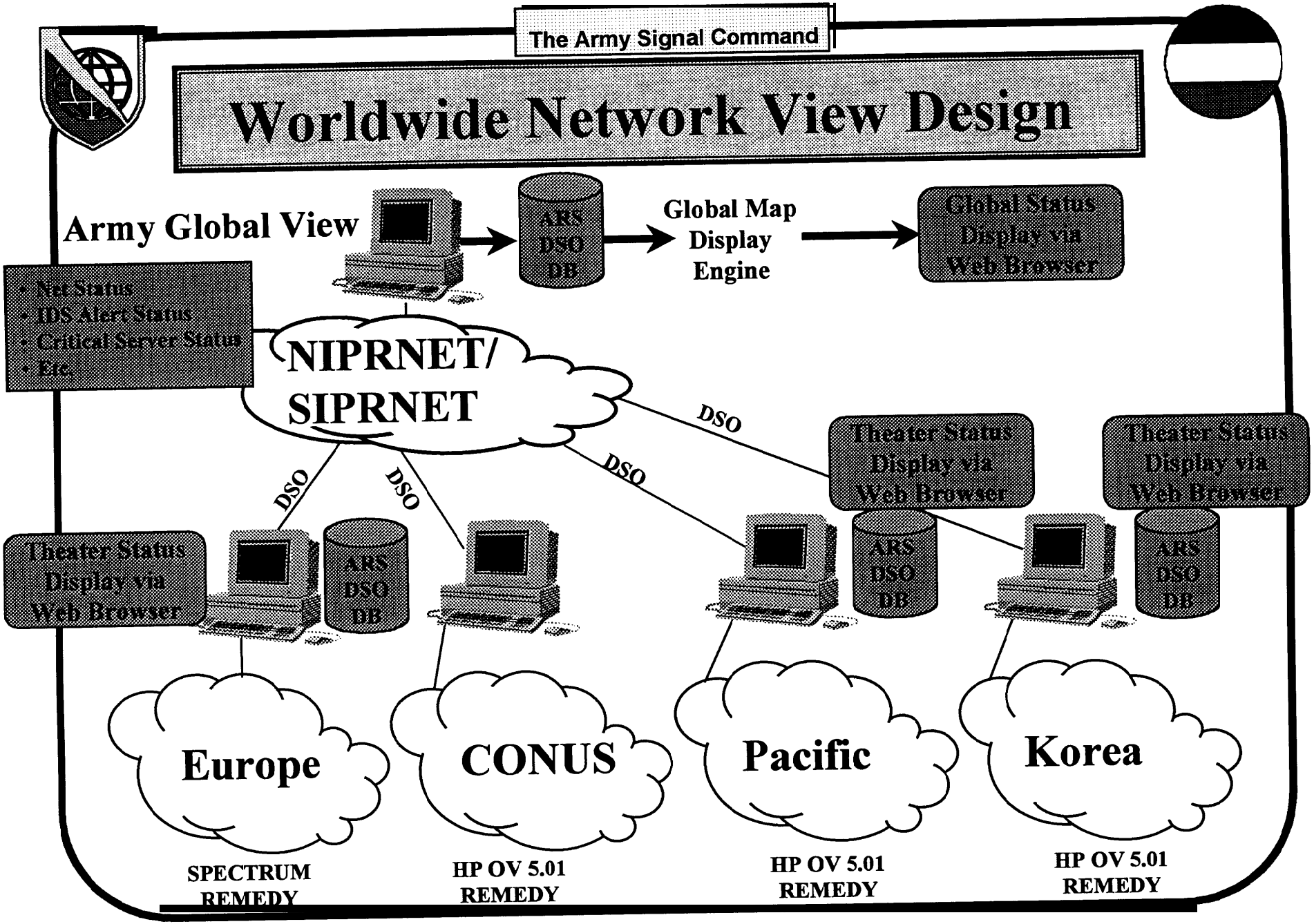
Organizational Concept of Operation (Unified CINC Perspective)



Basic Security Architecture

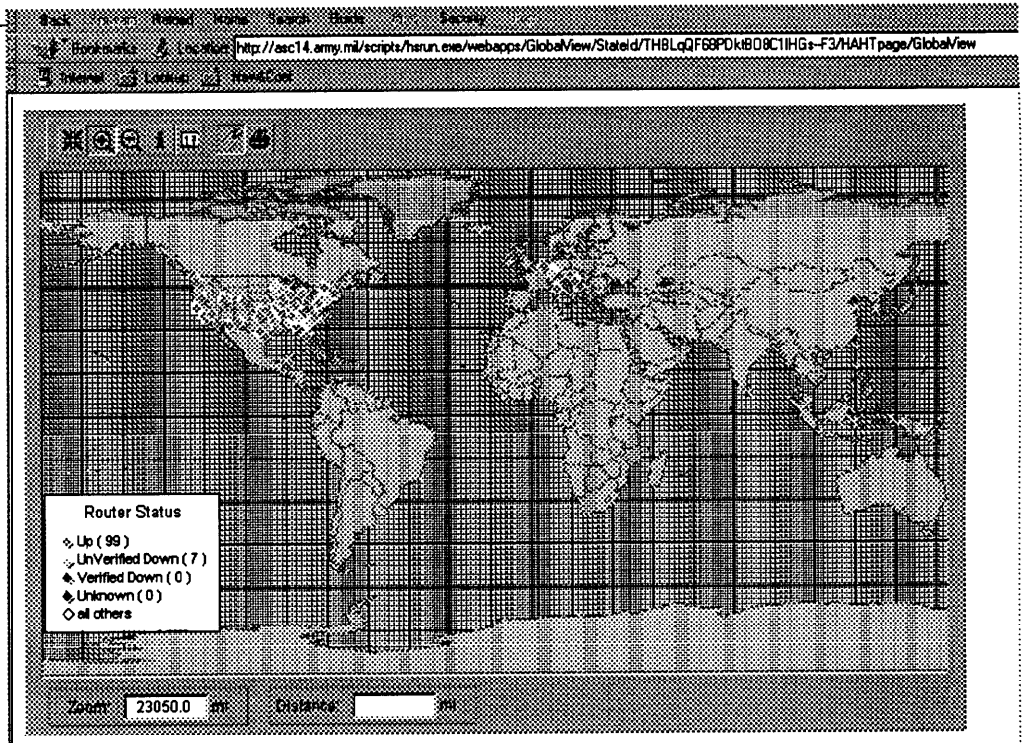


Worldwide Network View Design



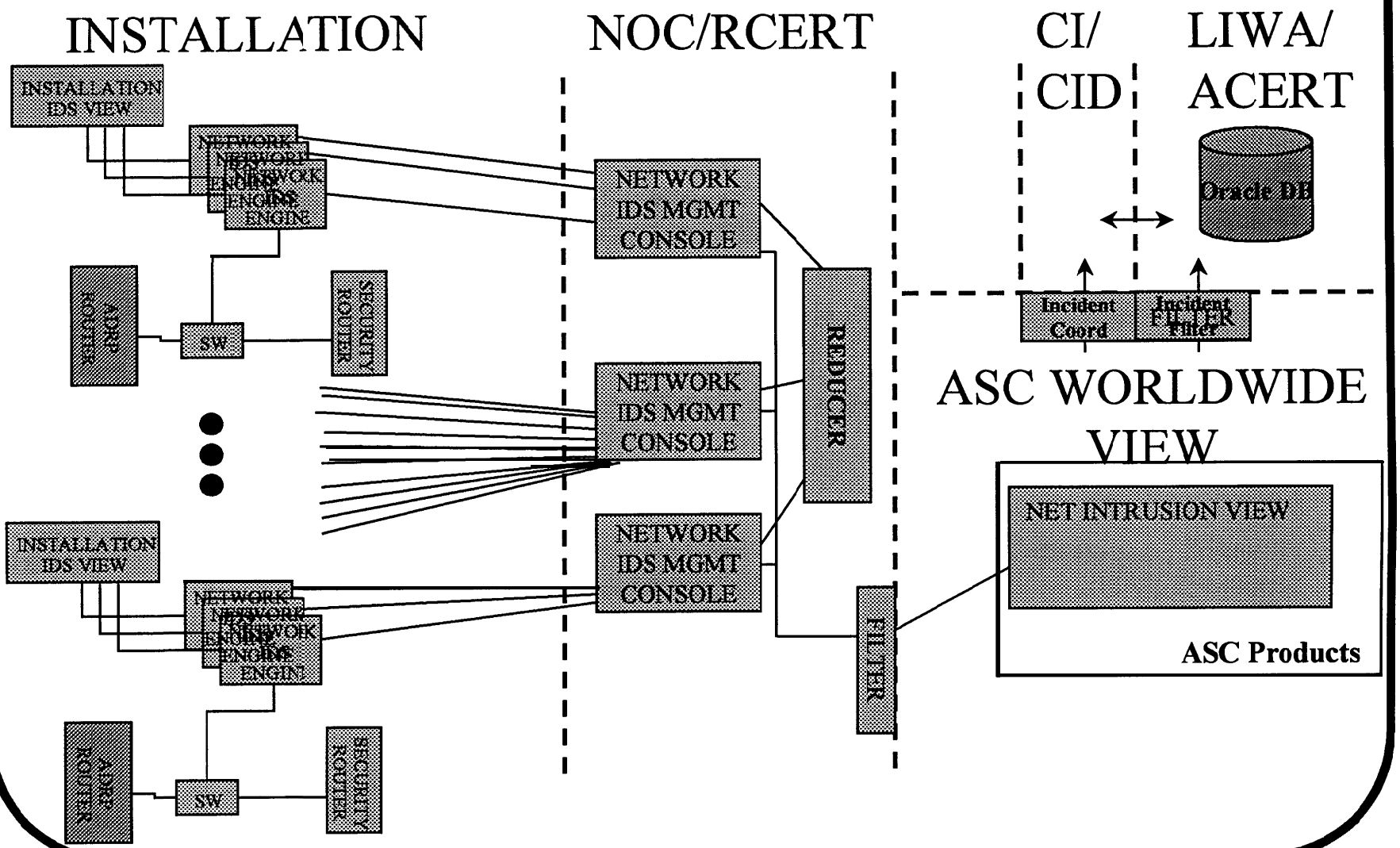
Worldwide Network View

- IOC: 15 July
  - Near Real Time view of CONUS and Europe NIPRNET
- FOC: 28 October
  - Near Real Time view of NIPRNET worldwide
  - Near Real Time view of SIPRNET worldwide

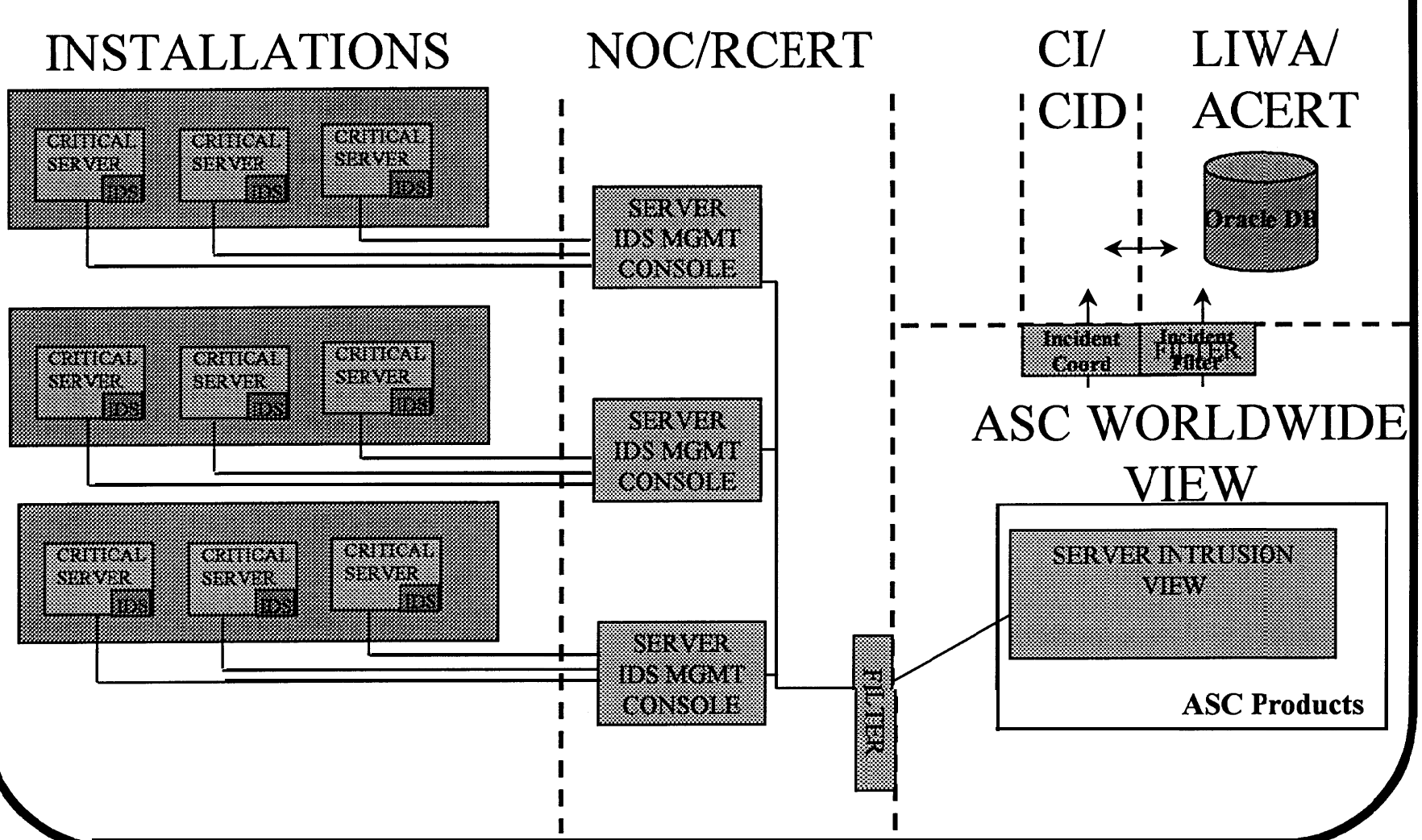


DATA IS CURRENT WITHIN 5-15 MINUTES

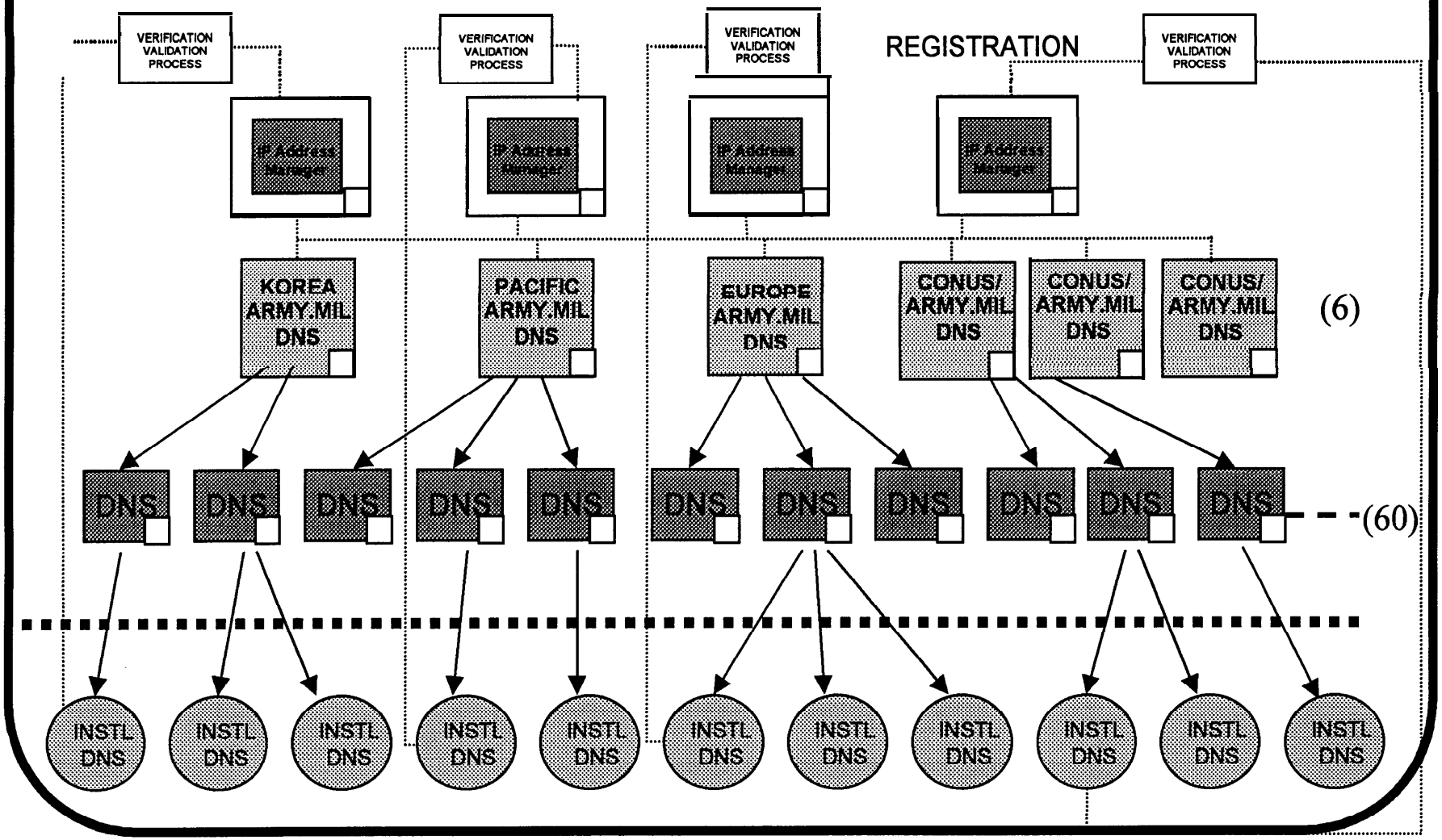
Network IDS Design



Server IDS Design

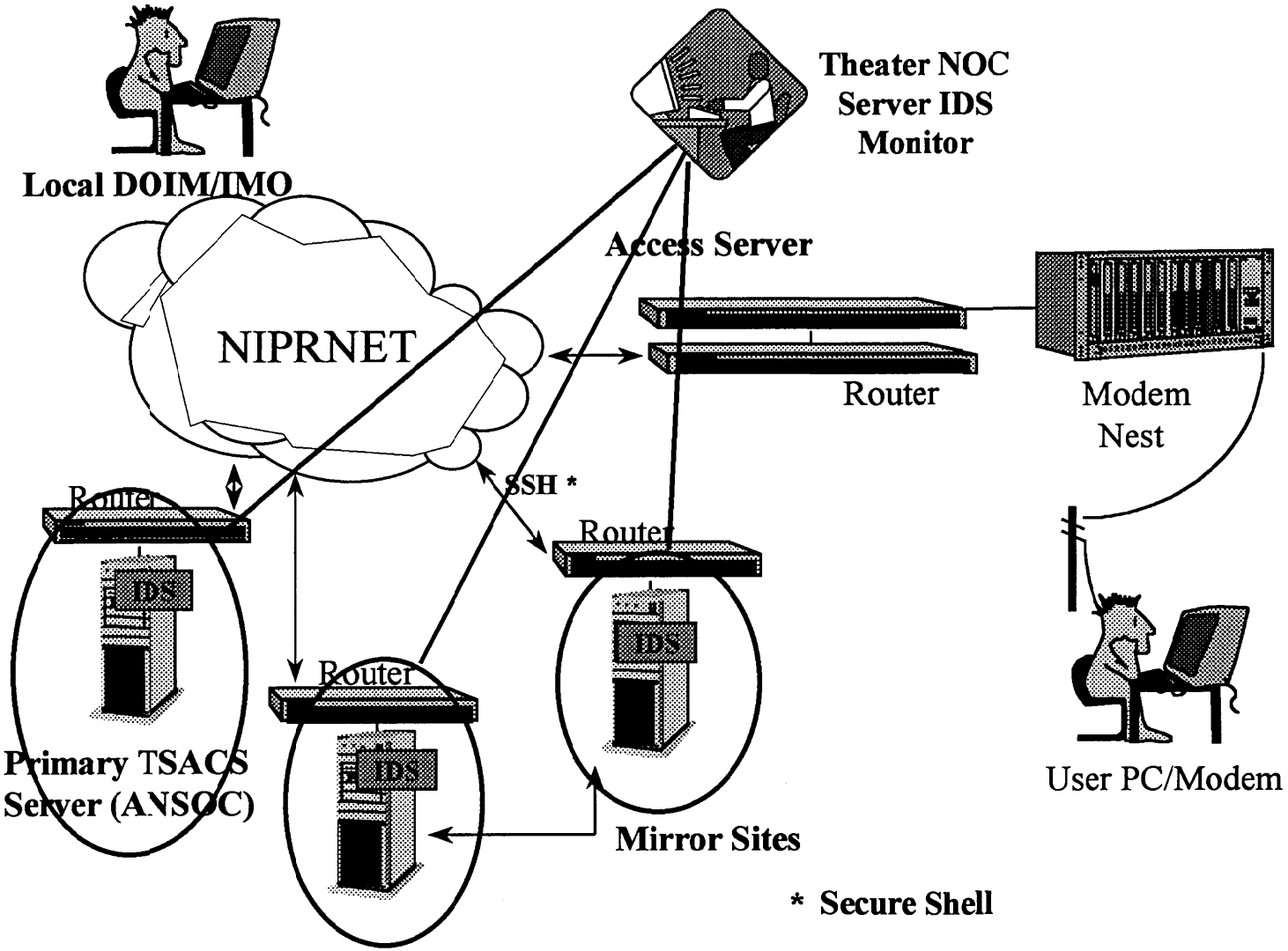


DNS Design



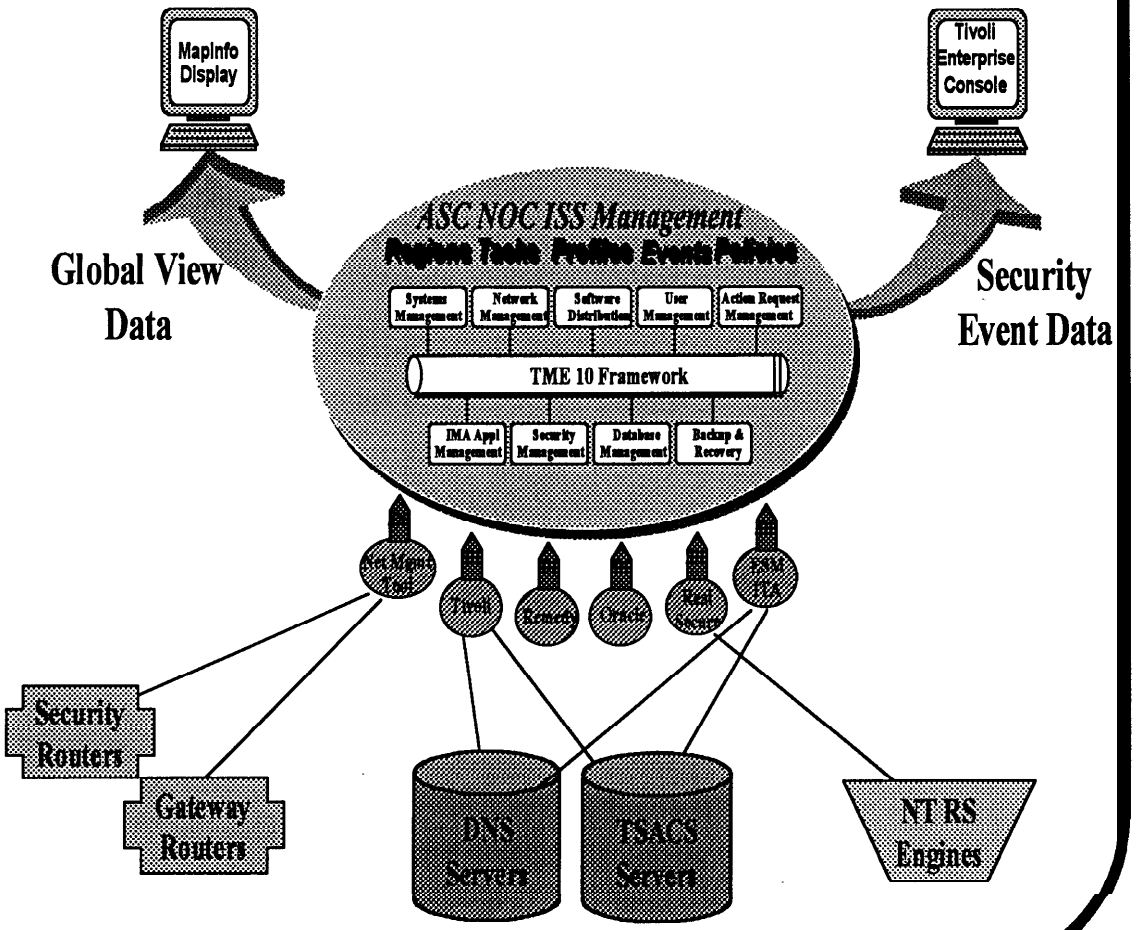
❑ =IDSS/WandTIVOLIClient

TSACS IDS (Server) Design

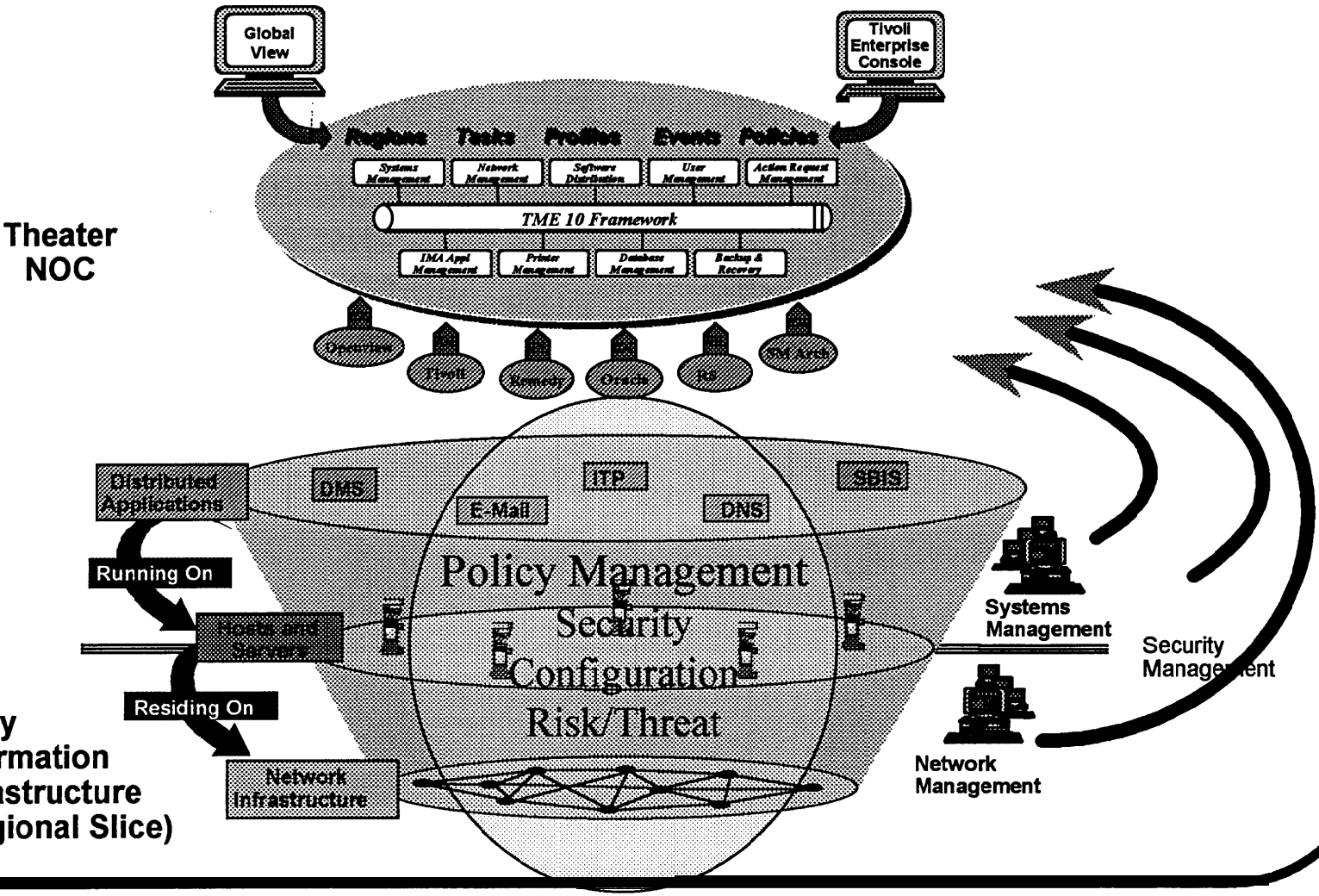


Centralize Management and Configuration Control

- IOC: 30 September
  - Centralized Access Control List Management of security router
- FOC: 27 November
  - Router configuration management
  - Configuration control of IDS engines & DNS servers
  - Configuration control Golden Master established
  - Configuration control board staffed with engineering support



ASC Integrated Management System - Circa 2000
The Common Framework Environment



CND R&D Thrusts
3 Main Areas

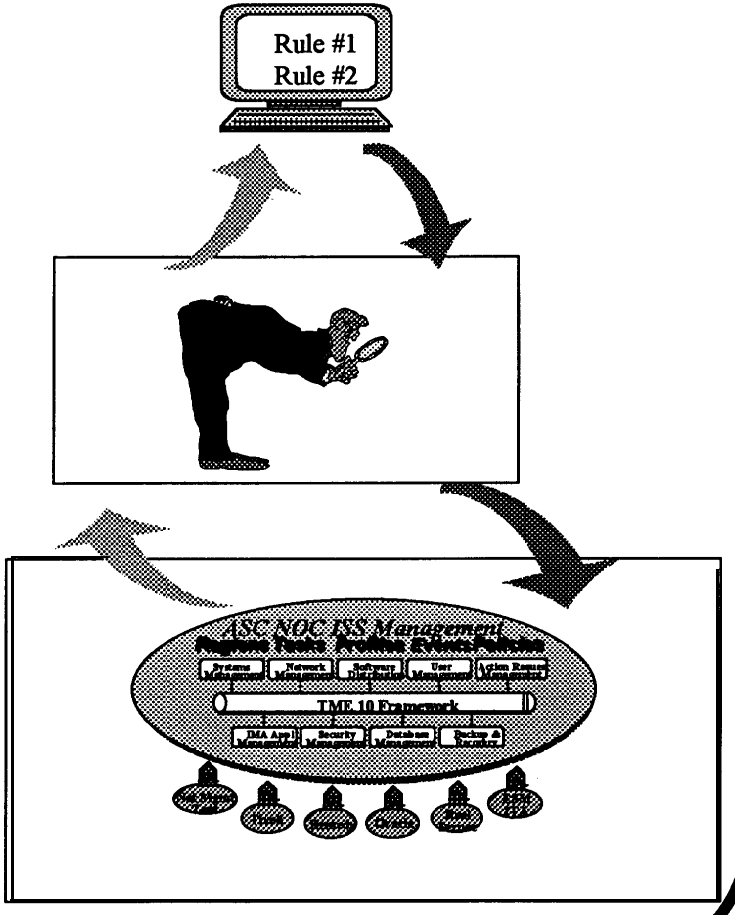
- Policy-driven Intelligent Agents for monitoring/ analysis of high volume event flows
- Improved Data Visualization techniques for more intuitive situational awareness
- Improved sensor technologies for monitoring high-speed data flows

Policy-driven Intelligent Agents

GUI based "Policy Manager" allows systems operators to establish management 'Policies" which are translated to "rules" for execution by Intelligent Agent objects

Intelligent Agents - Software Objects driven by rule-base continuously monitor the CIM and execute domain specific controls based on pre-defined rules

Common Information Management Environment - Object Oriented Framework provides a convergence of event infomation from a multitude of sensors within the enterprise into a single event store (database).



Intuitive Data Visualization

- Current data visualization techniques are either tabular event tables or simple graphs depicting topology relationships between objects
- Some objects are physical devices, others are logical constructs such as user accounts or databases - relationships between these objects are not easily discernible with current display technologies
- NOC Operators are being flooded with hundreds of thousands of events occurring on thousands of objects
- Current data visualization capabilities will not scale to the enormous flow of information that needs to be analyzed - More intuitive data visualization techniques are going to be essential to communicate true situational awareness and appropriate defensive responses

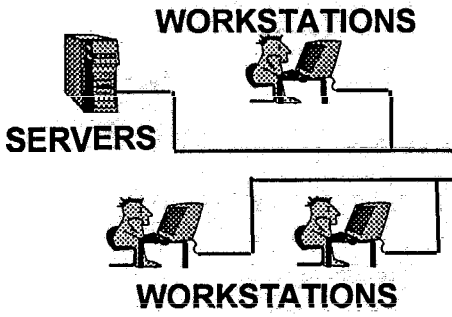
Improved Sensor Technologies

- Current IDS sensor technologies are not capable of operating effectively at available wire speeds such as ATM or Gigabit Ethernet
- As backbone network speeds continue to increase to nearly back-plane speeds the current IDS technologies threaten to become unacceptable bottle-necks on the information highway
- New technologies for improving security sensing capabilities have got to be developed

Network Security Improvement Pgm

Phase I

- Workstation and Server-based security
- ID and Passwords
- TCP Wrapper
- Security Scanning
- Anti-Virus

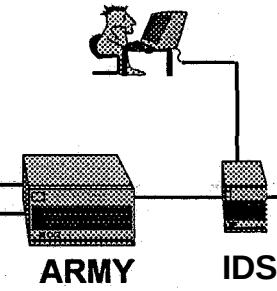


- Training
- World Wide Web Security
- NT Security
- Network Access Policy
- System Policies
- and More ....

Build Foundation

Phase II

- Intrusion Detection System Reporting to DOIM and CERTs
- Router-Based Security (Filtering)

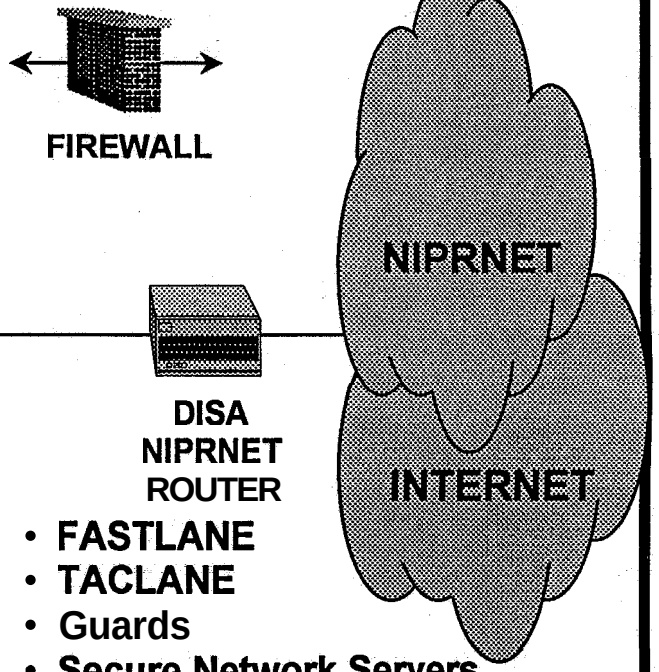


- Centralize Dial-In
- Re-Home Backside Connections
- Security Controls for ISDN Circuits
- Reconfigure Networks

Harden Infrastructure

Phase III

- Install Firewalls (If Needed For Specific Network Security Rqmts
- One-Time Passwords



- FASTLANE
- TACLANE
- Guards
- Secure Network Servers
- Public Key Infrastructure
- Latest technology

Insert New Technology

C2 Protect Conclusion

Army's initial C2P security architecture *in place*

Standardized systems architecture critical

Continuous effort required to improve our security posture